Universal Composable Password Authenticated Key Exchange for the Post-Quantum World

You Lyu[1,2], Shengli Liu[1,2](✉), and Shuai Han[2,3]

[1] Department of Computer Science and Engineering
Shanghai Jiao Tong University, Shanghai 200240, China
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[3] School of Cyber Science and Engineering, Shanghai Jiao Tong University,
Shanghai 200240, China
{vergil,slliu,dalen17}@sjtu.edu.cn

Abstract. In this paper, we construct the *first* password authenticated key exchange (PAKE) scheme from isogenies with Universal Composable (UC) security in the random oracle model (ROM). We also construct the *first* two PAKE schemes with UC security in the quantum random oracle model (QROM), one is based on the learning with error (LWE) assumption, and the other is based on the group-action decisional Diffie-Hellman (GA-DDH) assumption in the isogeny setting.

To obtain our UC-secure PAKE scheme in ROM, we propose a generic construction of PAKE from basic lossy public key encryption (LPKE) and CCA-secure PKE. We also introduce a new variant of LPKE, named extractable LPKE (eLPKE). By replacing the basic LPKE with eLPKE, our generic construction of PAKE achieves UC security in QROM. The LPKE and eLPKE have instantiations not only from LWE but also from GA-DDH, which admit four specific PAKE schemes with UC security in ROM or QROM, based on LWE or GA-DDH.

1 Introduction

Password Authenticated Key Exchange (PAKE) enables two parties (say, a client and a server) who possess a low-entropy password *pw* to securely establish session keys over public networks. These session keys subsequently facilitate the establishment of secure communication channels. Unlike authenticated key exchange (AKE), which necessitates a Public Key Infrastructure (PKI) to verify the authenticity of public keys, PAKE runs with easily memorable passwords and offers enhanced convenience for deployments and applications.

Security Notions for PAKE: IND vs. UC. There are two primary security notions for PAKE, the game-based security in the Indistinguishability model (IND security) [9] and the simulation-based security under the Universally Composable framework (UC security) [18]. As shown in [18], the UC security in the UC framework implies the IND security. In contrast to the IND model which assumes passwords uniformly distributed over a set, the UC framework permits